



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/614,087	07/11/2000	Robert C. Leah	RSW9-2000-0074-US1	1360

7590 01/27/2005

Gregory M Doudnikoff
IBM Corporation T81/062
P O Box 12195
Research Triangle Park, NC 27709

EXAMINER

TRAN, TONGOC

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 01/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/614,087

Applicant(s)

LEAH ET AL.

Examiner

Tongoc Tran

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 01 September 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-46 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-46 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

1. This office action is in response to Applicant's filing of Request for Continued Examination filed on 9/9/2004. Claims 1, 3-6, 12-, 18-19, 22, 24-27, 33-34, 39-40, 43-46 have been amended. Claims 1-46 are pending.

Response to Arguments

2. Applicant's arguments with respect to independent claims have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-17, 19-38 and 40-46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blakley, III et al. (U.S. Patent No. 5,862,323 hereinafter Blakley) in view of Barry et al. (U.S. Patent No. 6,615,258, hereinafter Barry).

In respect to claim 1, Blakley discloses a computing environment having a connection to a network, a computer program product for securely propagating security credentials using a trusted authenticating domain, the computer program product embodied on one or more computer-readable media and comprising computer-readable program code means for establishing a secure

connection between a client and a password synchronization agent (PSA) (see col. 3, lines 35-46);

computer-readable program code means for transmitting an identifier of a user and an identifying secret of the user from the client to the PSA over the secure connection

(see col. 2, lines 45 and col. 3, lines 35-46);

computer-readable program code means for validating the user with the trusted authenticating domain using the transmitted user identifier and identifying secret, on request of the PSA (see col. 2, line 26-57);

computer-readable program code means for propagating the identifying secret of the user directly from the PSA to a master registry if the validation succeeds (see Fig. 3A, col. 2, lines 24-col. 3, lines 20 and col. 6, lines 40-60 and col. 7, lines 7-33).

Blakley does not explicitly disclose but Barry discloses receiving at the PSA from the client over the secure connection during the propagation request processing and propagating the received identifying secret of the user directly from the PSA to a master registry (see Barry col. 12, line 63-col. 13, line 13, "e.g. user changes password, the new password is transmitted in real time to a server responsible for updating...").

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of Barry's real time propagating of user password with the teaching of Blakley for teaching of password synchronization between a main data store and a plurality of secondary data stores for more secure protection of the user identifier and identifying secret.

In respect to claim 2, Blakley and Barry disclose the computer program product according to Claim 1, further comprising:

computer-readable program code means for establishing a second secure connection between the PSA and the trusted authenticating domain; and

computer-readable program code means for using the second secure connection for the validating of the user (see col. 6, lines 22-34).

In respect to claim 3, Blakley and Barry disclose the computer program product according to Claim 1, further comprising:

computer-readable program code means for establishing a third secure connection between the PSA and the master registry (see col. 6, lines 22-34); and

computer-readable program code means for using the third secure connection for the propagating of the received identifying secret to the master registry (see col. 11 lines 27-31).

In respect to claim 4, Blakley and Barry disclose the computer program product according to Claim 1, further comprising computer readable program code means for propagating the received identifying secret to one or more other target registries if the validation succeeds (see col. 8, lines 34-44).

In respect to claim 5, Blakley and Barry disclose the computer program product according to Claim 4, further comprising:

computer-readable program code means for establishing additional secure connections between the PSA and each of the other target registries (see col. 8, lines 34-44); and

computer-readable program code means for using the additional secure connections for the propagating of the received identifying secret to the other target registries (see Col. 8, lines 34-44).

In respect to claim 6, Blakley and Barry disclose the computer program product according to Claim 11. further comprising:

computer-readable program code means for obtaining an identification of the trusted authenticating domain from the user during the propagation request processing (see Col. 5, line 49-col. 6, line 2);
and

computer-readable program code means for verifying that the trusted authenticating domain is trusted by the master registry as a prerequisite to the propagating (see Col. 3, line 54-60, Col. 6, lines 40-60).

In respect to claim 7, Blakley and Barry disclose the computer program product according to Claim 1, further comprising:

computer-readable program code means for obtaining an identification of the trusted authenticating domain from the master registry (see Col. 6, lines 40 60).

In respect to claim 8, Blakley and Barry disclose the computer program product according to Claim 6, wherein the master registry stores trust policy information. and wherein the computer-readable program code means for verifying that the trusted authenticating domain is trusted further comprises computer-readable program code means for checking whether the stored trust policy information for

the user includes the identification obtained from the user (see Col. 3, lines 54-60, Col. 5, line 49-col. 6, line 2 and Col. 6, lines 40-60).

In respect to claim 9, Blakley and Barry disclose the computer program product according to Claim 5, wherein the master registry stores trust policy information, and wherein the computer-readable program code means for verifying that the trusted authenticating domain is trusted further comprises computer-readable program code means for checking whether the stored trust policy information for a user group of which the user is a member includes the identification obtained from the user (see col. 6, lines 40-60).

In respect to claim 10, Blakley and Barry disclose the computer program product according to Claim 7, wherein the master registry stores trust policy information, and wherein the computer-readable program code means for obtaining the identification of the trusted authenticating domain from the master registry further comprises:

computer-readable program code means for obtaining the identification using the stored trust policy information for the user (see col. 3, lines 54-60, col. 6, lines 40-60).

In respect to claim 11, Blakley and Barry disclose the computer program product according to Claim 7, wherein the master registry stores trust policy information, and wherein the computer-readable program code means for obtaining the identification of the trusted authenticating domain from the master registry further comprises computer-readable program code means for obtaining the

identification using the stored trust policy information for a user group of which the user is a member (see col. 6, lines 40-60).

In respect to claim 12, Blakley and Barry disclose the computer program product according to Claim 4, wherein the master registry stores password synchronization policy information, and wherein the computer-readable program code means for propagating the received identifying secret to the one or more other target registries further comprises computer-readable program code means for identifying the one or more other, target registries using the stored password synchronization policy information for the user (see col. 8, lines 34-44).

In respect to claim 13, Blakley and Barry disclose the computer program product according to Claim 4, wherein the master registry stores password synchronization policy information, and wherein the computer-readable program code means for propagating the received identifying secret to the one or more other target registries further comprises computer-readable program code means for identifying the one or more other target registries using the stored password synchronization policy information for a user group of which the user is a member (see col. 7, lines 24-50).

In respect to claim 14, Blakley and Barry disclose the computer program product according to Claim 1, wherein the computer-readable program code means for establishing the secure connection further comprises computer-readable program code means for authenticating the PSA to the client (see col. 2, lines 34-45).

In respect to claim 15, Blakley and Barry disclose the computer program product according to Claim 2, wherein the computer-readable program code means for establishing the second secure connection further comprises computer readable program code means for authenticating the trusted authenticating domain to the PSA (see col. 2, lines 34-45).

In respect to claim 16, Blakley and Barry disclose the computer program product according to Claim 3, wherein the computer-readable program code means for establishing the third secure connection further comprises computer readable program code means for authenticating the master registry to the PSA (see col. 2, lines 34-45).

In respect to claim 17, Blakley and Barry disclose the computer program product according to Claim 5, wherein the computer-readable program code means for establishing additional secure connections further comprises computer readable program code means for authenticating the other target registries to the PSA (see col. 8, lines 34-44).

In respect to claim 19, Blakley and Barry disclose the computer program product according to Claim 1, wherein the computer-readable program code means for validating further comprises computer-readable program code means for invoking an authenticated LDAP bind or other native authentication mechanism of the trusted authenticating domain, wherein the received identifier of the user and the identifying secret of the user are passed to the trusted authenticating domain, thereby causing the trusted authenticating domain to validate the passed

Art Unit: 2134

identifier and identifying secret and return a result which reports a success or failure of the validation (see col. 7, line 52-col. 8, line 4).

In respect to claim 20, Blakley and Barry disclose the computer program product according to Claim 1, wherein the PSA has administrative authority for performing operations at the master registry (see col. 11, lines 27-31).

In respect to claim 21, Blakley and Barry disclose the computer program product according to Claim 4, wherein the PSA has administrative authority for performing operations at the one or more other target registries (see col. 3, lines 35-53).

In respect to claims 22-38 and 40-42, the claim limitations are system claims that are substantially similar to computer readable medium claims 1-17 and 19-21. Therefore, claims 22-38 and 40-42 are rejected based on the similar rationale.

In respect to claim 43, the claim limitation is a method claim that is substantially similar to computer readable medium claim 1. Therefore, claim 43 is rejected based on the similar rationale.

In respect to claim 44, Blakley and Barry disclose the computer program product according to claim 1, further comprising:

Computer-readable program code means for obtaining a new value from the user to be used as the propagated identifying secret if the validation succeeds (see col. 2, lines 15-54 and col. 7, lines 5-34); and

Computer-readable program code means for substituting this new value for the received identifying secret prior to operation of the computer-readable program code means for propagating (see col. 7, line 52-col. 8, line 4).

In respect to claims 45-46, the claim limitations are system and method claims that are substantially similar to computer-readable program code means of claim 1. Therefore, claims 45-46 are rejected based on the similar rationale.

4. Claims 18 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blakley (U.S. Patent No. 5,862,323) in view of Barry (U.S. Patent No. 6,615,258) and further in view of Huynh et al. (U.S. Patent No. 6,240,184).

In respect to claim 18 and 39, Blakley and Barry disclose the computer program product according to Claim 1, wherein the computer-readable program code means for validating further comprises:

computer-readable program code means for performing a security function on the received identifying secret of the user, wherein the security function comprises one of (i) a one-way hashing algorithm or (ii) an encryption algorithm (see col. 3, lines 9-19); computer-readable program code means for using the user identifier to locate a previously-stored identifying secret of the user which was stored by the master registry; and computer-readable program code means for comparing the located identifying secret to a result of performing the security function (see col. 2, lines 34-45).

Blakley and Barry do not disclose but Huynh discloses means for concluding that the validation succeeds if the located identified secret is identical to a result of

Art Unit: 2134

performing the security function (Huynh, col. 1, lines 14-54 and col. 2, lines 2745).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of Blakley and Barry's propagating plaintext password in real time with the teaching of Huynh's propagating encrypted password after validating of encrypted password succeeds so that attacker who gains access to the encrypted password can not readily discern the password (Huynh, col. 1, lines 34-37).

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

-Dietterich et al. disclose a dynamic directory service.

-Broomhall et al. disclose a client account generation and authentication system for a network service.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (571) 272-3843. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.


Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Examiner: Tongoc Tran
Art Unit: 2134

TT

January 21, 2005


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100